IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF VIRGINIA
Harrisonburg Division

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH **THEWLOUNGEBAR@GMAIL.COM** THAT IS STORED AT PREMISES CONTROLLED BY **GOOGLE, LLC.**	Case No. 5:20mj00016 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Tami Ketcham, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises controlled by Google, LLC ("Google"), an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the United States Immigration and Customs Enforcement, Homeland Security Investigations ("HSI"), and have been since 2010. I am currently assigned to the HSI office in Harrisonburg, VA. I have a bachelor's degree in Psychology and Sociology and a master's degree in Criminology. I am authorized to conduct criminal

investigations on behalf of HSI. During my employment with HSI, I have participated in the execution of subpoenas, search warrants, and arrest warrants, and have investigated various federal violations, including offenses pertaining to child exploitation and child pornography. Through such investigations, I have reviewed numerous examples of child pornography (as defined in 18 U.S.C. §2256) in various forms of media. My duties include, but are not limited to, investigations pertaining to Title 18 of the United States Code. I am a graduate of the Federal Law Enforcement Training Center's Criminal Investigator Training Program and have also received additional HSI investigative training, some of which has been related to conducting child exploitation and child pornography investigations. I previously worked as a Juvenile Probation Officer with the Florida Department of Juvenile Justice and during a portion of my employment I supervised a case load of juvenile sex offenders.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The information contained in this affidavit comes from my training and experience, my review of records, my direct observations, and through information obtained from other law enforcement officers.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18 U.S.C. §§ 2251 and/or 2252 have been committed by the user of thewloungebar@gmail.com. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States…that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

6. Kik Messenger ("Kik") is a mobile messaging application that can be used on both Androids and iPhones that uses an existing Wi-Fi connection or data plan to communicate with other users. The application can be used to send text messages, pictures, and videos. Users can communicate directly with an individual or with multiple users in a group chat. As a safety measure of Kik, users can only be logged into one device per an account at a time. When signing up for a Kik account, the following is collected: first and last name (not verified), desired Kik username (unique identifier and cannot be changed), email address (verified but not required), password, birthday (not verified), and phone number (not verified). A user-supplied email address at sign-up does not have to be verified but does result in an activation email being sent by Kik to the supplied email address. The user must then click on the activation email from the supplied email account in order to activate the Kik account.

7. Based on my training and experience, I know that Kik has been used to facilitate, distribute, access, view, find, and discuss child pornography. This is accomplished by individuals creating groups or finding other Kik users interested in child pornography. Child pornography is shared within Kik by users posting the images or videos of child pornography directly to the group

or providing a "link," which will direct the Kik user to various online storage sites where the images and videos of child pornography are stored.

8. HSI received lead information from the Royal Canadian Mounted Police that originated from the Legal Department at Kik Interactive indicating that on August 2, 2019 at 22:36:26 UTC, user wllovemsmth uploaded an image of what appeared to be a naked prepubescent male child lying on a bed with his arms outstretched; the child's genitals were exposed and were the focus of the image. The Kik account that uploaded the child pornography image was registered on July 24, 2019 at 00:53:14 UTC, and the registration device was an iPhone. The letter W was registered to the account as the user's first name and the letter L was registered to the account at the user's last name. The email address registered to the account was theWloungebar@gmail.com. Upon activation of the Kik account, Kik would have sent an email to theWloungebar@gmail.com with a notification indicating a new Kik account was created. An Internet Protocol (IP) address associated with account logins was IP 98.249.57.29.

9. Twitter is a social networking microblogging service that can be used with personal computers and cellular phones to include androids and iPhones. Twitter is a service that allows registered members to create their own profile pages and broadcast posts called tweets that can include photographs and videos. Twitter users may restrict their tweets to individuals whom they approve. Twitter users may also send private messages to one another through Direct Messages. Twitter users may be followed, and they may follow other twitter users. When signing up for a Twitter account, a user supplies a name, a phone number or email address, and a date of birth. When a user supplies a phone number upon activation, a text verification code is sent to the supplied phone number via text message. When a user supplies an email address upon activation,

a verification code is sent via email to the supplied email address. The verification code must be entered into Twitter to complete the activation of the Twitter account.

10. Based on my training and experience, I know that Twitter has been used to facilitate, distribute, access, view, find, and discuss child pornography. This is accomplished by individuals finding other Twitter users interested in child pornography. Child pornography can be shared within Twitter by users posting the images or videos of child pornography or by providing a "link," which will direct the Twitter user to various online storage sites where the images and videos of child pornography are stored. Users may also share child pornography privately by sending messages, photographs, and videos via Direct Messages to other specified users.

11. Harrisonburg Police Department ("HPD"), which is a part of the Northern Virginia Internet Crimes Against Children Task Force ("NOVA ICAC"), received National Center for Missing and Exploited Children ("NCMEC") CyberTipline Report No. 57143145 that contained information submitted by Twitter, Inc./Vine.co ("Twitter"). The tip was in reference to at least one image that was identified as child pornography that was uploaded on October 14, 2019 and sent by a user utilizing Twitter username AJBoylv. This Twitter account was registered on August 18, 2019 at 21:58:38 UTC. Your affiant reviewed the image, which appears to be of a prepubescent male child lying in the back seat of a vehicle with his legs spread apart. The child was unclothed from the waist down, and his genitals were the focus of the image. The name AJBoylv was registered as the account's screen/username and the user provided the description "Fun Masc guy loving life. Gym sports bling. Into kink." The email address registered to the Twitter account was theWloungebar@gmail.com. Upon activation of the Twitter account, Twitter would have sent an email to theWloungebar@gmail.com with a verification code that had to be entered into Twitter

to complete the activation of the Twitter account. An internet IP address associated with account login was IP 98.249.57.29. This is the same IP address associated with the uploading of child pornography on Kik on August 2, 2019.

12. A Virginia State Police Special Agent with the NOVA ICAC submitted a subpoena to Google requesting subscriber information and IP logs for the email address theWloungebar@gmail.com. The following subscriber information was included in the subpoena return information received from Google:

> Name-Rod Williams
> Email-thewloungebar@gmail.com
> Services-Gmail, Google Calendar, Location History, Minutemaid
> Recovery Email-Rodney@820sold.com
> Created On-2019/07/23-17:30:14 UTC
> Terms of Service IP-98.249.57.29 on 2019/07/23 17:30:14 UTC
> Google Account ID-174338791655

13. A Virginia State Police Special Agent with the NOVA ICAC submitted a subpoena to Comcast, which was the identified provider for IP address 98.249.57.29. The following subscriber information was included in the subpoena return information received from Comcast:

> Name-Derek Jackson
> Address-511 Paul Street, Harrisonburg, VA 22801

14. HPD identified Rodney Williams as the owner of 511 Paul Street, Harrisonburg, VA 22801, and Derek Jackson as a resident at the same address. In January 2020, HPD obtained and executed a search warrant at 511 Paul Street, Harrisonburg, VA 22801, during which time they encountered Rodney Williams. During the interview Williams stated:

a. Williams, Williams' wife, and Derek Jackson all reside at the home located on Paul Street. Per Williams, Derek Jackson rents the upstairs bedroom and has resided in

the home for approximately five years (in contradiction to Jackson's statement, below).

b. He confirmed he and his wife use Apple products (the Kik account was created by an iPhone).

c. Williams admitted that he created the email account wloungebar@gmail.com and it had been active for years (in contradiction to subscriber records obtained from Gmail that revealed the email account was created on July 23, 2019 at 17:30:14 UTC, which was approximately eight hours before the Kik account associated with user wllovemsmth was registered).

d. He had a Twitter account (Rodney820.sold) that he used for business but he rarely made any posts.

e. He reported that many people are in an out of the home, to include friends and guests that stay at his Airbnb that is located downstairs in the home. Williams reported there was guest access to the home internet that he shared with a lot of people that attended parties and events in his home.

f. He permitted his friends and Airbnb guests to use his iPad, from which they could access the email account wloungebar@gmail.com.

g. The current iPad in the Airbnb is relatively new. Williams threw away the previous iPad because it could no longer accept updates. Law enforcement informed Williams that the person that created the Twitter account in question would have had to have access to the email account wloungebar@gmail.com to confirm the

Twitter account when it was created. Williams reported it would have had to have taken place on the previous iPad as the email account was located on that iPad.

h. He denied communicating with minors or younger males on any platform.

i. Williams initially told law enforcement he was in possession of his Apple cellular phone; however, he later reported that he could not locate the phone, so law enforcement was unable to seize the phone during the execution of the search warrant.

15. Derek Jackson was at work and not present at the Paul Street address at the time of the execution of the search warrant. Two HPD detectives left the search warrant and met with Derek Jackson at his place of employment. During the interview, Jackson stated:

a. He has lived at the Williams home since 2004 and he uses his laptop or his phone when he is there.

b. He only the Twitter account (drjac0316) that he created in June or July of last year but he only uses it to follow Dolly Parton, Lady Gaga, and Rodney.

c. Jackson reported an Airbnb was being operated at the Williams home, and, prior to the creation of the Airbnb, parties were held in the Airbnb location during which time friends had access to an iPad. Jackson stated he, Williams, and Williams' wife all had access to the iPad.

d. Jackson reported he did not know who had access to the email account associated with the iPad, but he never had access to the account.

e. Jackson checked the Airbnb schedule and it appeared that different groups of people were present in the Airbnb when the Twitter account was created and

accessed, indicating the person who created the Twitter account in August 2019, accessed the account multiple times in September 2019 and October 2019, and uploaded the child pornography in October 2019 would likely have been a person that lived in the home.

f. Jackson consented for HPD to conduct an extraction on his Android cellphone. Law enforcement has reviewed the contents of the Android cellphone, which indicates no access to the email account wloungebar@gmail.com, nor any use of a Twitter account AJBoylv, nor any use of a Kik account.

16. On February 28, 2020, HPD submitted a preservation request to Google requesting information be preserved for the email account theWloungebar@gmail.com that was associated with both the Kik and Twitter accounts that were used to upload images of child pornography. HPD also requested information in Google Drive associated with the email account also be preserved.

GOOGLE

17. Through my training and experience, I have learned that Google provides a variety of on-line services, including electronic mail ("email") access, to the general public. Google allows subscribers to obtain email accounts at the domain name Google, like the email account listed in Attachment A. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. The computers of Google are likely to contain stored electronic communications (including retrieved and un-retrieved email for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account

application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

18. In general, an email that is sent to a Google subscriber is stored in the subscriber's "mail box" on Google servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Google servers indefinitely.

19. Emails stored in a subscriber's mail box may contain information pertaining to new social media and/or cellular phone application accounts that were created such as emails stored in a subscriber's mail box may contain account activation emails that require verification to create new social media and/or cellular phone application accounts. Such account activation emails can indicate that the subscriber of the email account received notification and/or verified the creation of new social media and cellular phone application accounts such as Kik and Twitter. This is particularly important if such new social media and/or cellular phone application accounts were used to conduct illicit activities.

20. When the subscriber sends an email, it is initiated at the user's electronic device, transferred via the Internet to Google's servers, and then transmitted to its end destination. Google often saves a copy of the email sent. Unless the sender of the email specifically deletes the email from the Google server, the email can remain on the system indefinitely.

21. Subscribers to Google might not store on their home computers copies of the emails stored in their Google account. This is particularly true when they access their Google account through the web, or if they do not wish to maintain particular emails or files in their residence. A Google subscriber can also store files, including emails, address books, contact or buddy lists,

pictures, and other files, on servers maintained and/or owned by Google including updating many functions, applications, and drives on Google's cloud storage system, Google Drive.

22. Google Drive is a cloud storage and synchronization service developed by Google. Google Drive allows users to store files on its servers, synchronize files across devices, and share files. In addition to a website, Google Drive offers apps with offline capabilities for Windows and macOS computers as wells as Android and iOS smartphones and tablets. A person may sign up for Google Drive, Gmail, Google Photos, and other Google services by creating a Google account, which provides the account user with 15 gigabytes of free cloud storage. The Google Photos app automatically sends photos to Google Drive. The Google Photos app can also automatically delete photos on your phone that have already been uploaded to Google Drive. A Gmail user is able to store email attachments sent through Gmail directly to their Google Drive. In my training and experience I am aware people may save photographs received in email attachments to their cloud storage such as Google Drive. I am also aware that images of child pornography have been found in cloud storage such as Google Drive. This information may provide clues to the subscriber's identity, location, or illicit activities.

23. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute

evidence of the crimes under investigation because the information can be used to identify the account's user or users.

24. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contact lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). This geographic information may tend to either inculpate or exculpate the account owner. Last, stored electronic data may provide relevant insight into the email account user's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the user's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

25. In my training and experience, evidence of who was using an e-mail account may be found in address books, contact or buddy lists, e-mail in the account, cloud services (Google Drive) and attachments to e-mails, including pictures and files.

CONCLUSION

26. Based on the forgoing, I request that the Court issue the proposed search warrant.

27. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Google, LLC. Because the warrant will be served on Google, which will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING

28. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

OATH

The information in this affidavit is true to the best of my knowledge and belief.

Respectfully submitted,

s/Tami Ketcham
Special Agent – ICE/HSI

Received by reliable electronic means and sworn and attested to by telephone on this 7th day of April 2020.

Joel C. Hoppe
JOEL C. HOPPE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with theWloungebar@gmail.com and Google Account Identification 174338791655 that is stored at premises owned, maintained, controlled, or operated by Google, LLC., a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google, LLC. ("Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for the account or identifier listed in Attachment A:

a. All records and information associated with the account listed in Attachment A for the following as applicable: Gmail, Web History, Google Search History, Location History, Google Photos, Google Docs, Google Calendar, Google Maps, and Google Drive;

b. All Internet search requests inputted by the subscriber for the account listed in Attachment A and URLs and/or IP addresses typed into the web browser's address bar or URLs and/or IP addresses clicked on for the account listed in Attachment A;

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, deleted emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

d. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP

address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

e. The types of service utilized;

f. All records or other information stored by an individual using the account, including address books, contact and buddy lists, Google Calendar, Google Wallet/Finance, pictures to include exif data, and any other files;

g. All records pertaining to devices from which the account accessed and Google services or which any Google service is synced, to include device serial numbers, model type/number, IMEI, and MAC address;

h. Information regarding network identifiers from which any Google service was accessed, to include IP addresses and associated date and time of access; and

i. All stored communications or files including the Gmail account and contents of Google Drive accounts including backup of applications and accounts; and

j. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within **14 days** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of **18 U.S.C. §§ 2251 and 2252**, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) Communications to and from Twitter, Kik, and other electronic services providers that can be used to receive, distribute, and possess child pornography.

(b) Possession, receipt, and production of child pornography;

(c) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the Google account owner;

(d) Evidence indicating the Google account owner's state of mind as it relates to the crime under investigation;

(e) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

(f) The identity of the person(s) who communicated with the user ID about matters relating to the receipt or distribution of child pornography, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communication, other records and information disclosed pursuant to this warrant in order to located evidence, fruits, and instrumentalities described in the warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support

staff, and technical experts. Pursuant to this warrant, HSI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.